DIMENSION OF $H_1(X_1(p), C_1^0, \mathbb{Z}_p)^+$ VIA MANIN SYMBOLS

R. SCOTT WILLIAMS

Contents

1. Introduction

Fix a prime $p \geq 5$ and let C_1^0 denote the nonzero cusps on the modular curve $X_1(p)$. We know that the dimension of $H_1(X_1(p), C_1^0, \mathbb{Z}_p)^+$ is given by the sum of the genus of $X_1(p)$ and the size of C_1^0 minus 1. By a result of Shimura (Prop. 1.40, [Shi71]) we know that for $p \geq 5$ the genus is

$$g = \frac{(p-5)(p-7)}{24},$$

and an easy computation show that $|C_1^0| = \frac{p-1}{2}$. Thus,

$$\dim H_1(X_1(p), C_1^0, \mathbb{Z}_p)^+ = \frac{(p-5)(p-7)}{24} + \frac{p-1}{2} - 1 = \frac{p^2-1}{24}.$$

In this paper we seek to compute this dimension in another manner – via Manin symbols.

We proceed now using the definitions and notation found in [Sha06]. For $u, v \in \mathbb{Z}/p\mathbb{Z}$, define

$$[u : v] = \left\{ \frac{a}{pc}, \frac{b}{pd} \right\}$$

to be the class of the geodesic from $\frac{a}{pc}$ to $\frac{b}{pd}$, where $a, b, c, d \in \mathbb{Z}$ are such that $ad - bc = 1$, $u \equiv a \pmod{p}$ and $v \equiv b \pmod{p}$. These symbols are the usual Manin symbols with the Atkin-Lehner involution applied, and we will simply refer to them as Manin symbols.

Let D denote the group $(\mathbb{Z}/p\mathbb{Z})^\times$ of diamond operators on $H_1(X_1(p), C_1^0, \mathbb{Z}_p)$, then $H_1(X_1(p), C_1^0, \mathbb{Z}_p)$ has a presentation as a $\mathbb{Z}_p[D]$-module with generators $[u : v]$ subject to the relations:

$$[-u : -v] = [u : v] \tag{1.1}$$

$$[u : v] + [-v : u] = 0 \tag{1.2}$$

$$[u : v] - [u : u + v] - [u + v : v] = 0. \tag{1.3}$$

Taking the plus part of $H_1(X_1(p), C_1^0, \mathbb{Z}_p)$ then produces the following extra relation:

$$[u : v] - [-u : v] = 0. \tag{1.4}$$

Using relations (1.1) – (1.4), if we can compute the minimum number of symbols necessary to generate $H_1(X_1(p), C_1^0, \mathbb{Z}_p)^+$ we will have another method of computing the dimension.

2. Using the Relations

We begin with $u, v \in \mathbb{Z}/p\mathbb{Z}$ meaning that initially there are p^2 symbols, $[u : v]$, generating $H_1(X_1(p), C_1^0, \mathbb{Z}_p)^+$; however, using relations (1.1) – (1.4) we can greatly reduce this number. First, since we are considering only nonzero cusps we have that $u, v \neq 0$, and by (1.1), $[u : v] = [-u : v]$ tells us $0 < u \leq \frac{p-1}{2}$.

For notations sake, we combine relations (1.2) and (1.4) to see that

$$[u : v] = -[-v : u] = -[v : u], \tag{2.1}$$

and if we use (1.2) twice followed by (1.4) we have

$$[u : v] = -[-v : u] = [-u : -v] = [u : -v]. \tag{2.2}$$

Hence, similar to what we showed above, (2.2) implies $0 < v \leq \frac{p-1}{2}$. We note now that by (2.1),

$$[u : u] = -[u : u],$$

which implies that $[u : u] = 0$, i.e., $[u : v]$ with $u = v$ is not a generator. (We note here also that by (1.4) this implies $[-u : u] = 0$.) So, without loss of generality, we may assume $u \neq v$ which gives us

$$0 < u < v \leq \frac{p-1}{2}.$$

From this point forward we will simply write $u < v \leq \frac{p-1}{2}$ with the understanding that u is nonzero. We will further assume that, unless specifically stated, these inequalities hold throughout the remainder of the paper.

Now we take care in investigating relation (1.3):

$$[u : v] = [u : u + v] + [u + v : v].$$

To do so, we must consider four cases:

(1) $\boldsymbol{u \equiv -2v \pmod{p}}$ **:** The condition $u \equiv -2v \pmod{p}$, by the assumption that $u < v \leq \frac{p-1}{2}$, is equivalent to the condition that $u + 2v = p$. In this case, we see that

$$[u : v] = [-2v : v] \overset{(1.3)}{=} [-2v : -v] + [-v : v] \overset{(2.2)}{=} [-2v : v],$$

which gives us no relation among the symbols.

(2) $\boldsymbol{v \equiv -2u \pmod{p}}$ **:** Similar to case (1), this condition is equivalent to $2u + v = p$, and we see that

$$[u : v] = [u : -2u] \overset{(1.3)}{=} [u : -u] + [-u : -2u] \overset{(1.4)}{=} [u : -2u],$$

again giving no relation among the symbols.

Before moving on to our final two cases, we set a notational convention. In order to apply relation (1.3) we stipulate that all symbols must be written such that each entry is less than or equal to $\frac{p-1}{2}$, if an entry is larger than this value, we must replace it with its negative.

In addition, in the following two cases we see to determine whether, for a fixed u, v, relation (1.3),

$$[u : v] = [u : u + v] + [u + v : v],$$

or a permutation of it, appears more than once after applying (1.3) to all other symbols. However, since we know which terms must appear in the relation, it suffices to check the result of applying (1.3) to both $[u : u + v]$ and $[u + v : v]$.

(3) $\boldsymbol{u + v \leq \frac{p-1}{2}}$ **:** We first note that since $u + v \leq \frac{p-1}{2}$, we will not have to replace $u + v$ by its negative before applying relation (1.3). Applying (1.3) to $[u : u + v]$ we see

$$[u : u + v] = [u : 2u + v] + [2u + v : v]$$

Since we know $[u : u + v] = [u : v] - [u + v : v] = [u : v] + [v : u + v]$ from the "usual" relation (with the second equality coming from relation (2.1)), we need to determine whether these two relations involving $[u : u + v]$ are distinct.

If the relations were equivalent, we would have either

$$[\pm u : \pm(2u + v)] = [\pm u : \pm v] \text{ and } [\pm(2u + v) : \pm v] = [\pm v : \pm(u + v)] \tag{2.3}$$

or

$$[\pm u : \pm(2u + v)] = [\pm v : \pm(u + v)] \text{ and } [\pm(2u + v) : \pm v] = [\pm u : \pm v]. \tag{2.4}$$

We note that by relations (1.2) and (1.4), we can replace any symbol $[u : v]$ by either $[-u : v], [u : -v]$, or $[-u : -v]$, which makes the $\pm$'s above necessary.

Examining (2.3) we see that for equality to hold, we would need $\pm v = \pm(u + v)$; however, by assumption, $0 < u < p$ so this is impossible. Hence, (2.3) cannot hold. As for (2.4), we also have assumed that $u \neq v$, so we cannot have $\pm u = \pm v$, and thus (2.4) does not hold. Therefore, the relation $[u : u + v] = [u : 2u + v] + [2u + v : v]$ is a distinct relation from $[u : u + v] = [u : v] + [v : u + v]$.

Using a similar argument one can show that $[u + v : v] = [u + v : u + 2v] + [u + 2v : v]$ is distinct from $[u + v : v] = [u : v] + [u + v : u]$. Hence, for a fixed symbol $[u : v]$ with $u + v \leq \frac{p-1}{2}$, applying relation (1.3) gives a unique relation among all other symbols.

(4) $\boldsymbol{u + v > \frac{p-1}{2}}$ **:** Similar to case (3) we will apply relation (1.3) to the symbols $[u : u + v]$ and $[u + v : v]$; however, since $u + v > \frac{p-1}{2}$, we must first replace $u + v$ by $-(u + v)$. Hence, we see that

$$\begin{aligned} [u : u + v] = [u : -(u + v)] &= [u : -v] + [-v : -(u + v)] \\ &= [u : v] - [u + v : v], \end{aligned}$$

with the last equality following from relations (2.2), (1.1) and finally (2.1). Clearly the relation obtained by applying (1.3) to $[u : u + v]$ is equivalent to the "usual" relation from (1.3) applied to $[u : v]$.

Also, applying (1.3) to $[u+v:v]$ yields:

$$\begin{aligned}[u+v:v] = [-(u+v):v] &= [-(u+v):-u] + [-u:v] \\ &= -[u:u+v] + [u:v],\end{aligned}$$

which is again equivalent to the "usual" relation.

Hence, applying relation (1.3) to any of $[u:v], [u:u+v]$, and $[u+v:v]$ with $u+v > \frac{p-1}{2}$ will produce the same relation between symbols.

3. Formula for Number of Generators

In the previous section we saw that for a symbol $[u:v]$, if $u+v \leq \frac{p-1}{2}$ then relation (1.3) would produce a unique relation among all symbols, which allows us to eliminate one symbol, say $[u:v]$, from our set of necessary generators.

On the other hand, if $u+v > \frac{p-1}{2}$, then relation (1.3) would produce the same relation for $[u:v], [u:u+v]$, and $[u+v:v]$. Additionally, if $v \equiv -2u \pmod p$ or $u \equiv -2v \pmod p$, then relation (1.3) provided no relation at all. Since these two cases are equivalent to $2u+v=p$ and $u+2v=p$, respectively, we see that if $v = p-2u$ then

$$u+v = p-u \geq p - \left(\frac{p-1}{2} - 1\right) = \frac{p+1}{2} > \frac{p-1}{2},$$

and if $u = p-2v$ we first note $v < \frac{p-1}{2}$ (since if $v = \frac{p-1}{2}$ then it would have to be the case that $u=0$) and so

$$u+v = p-v \geq p - \left(\frac{p-1}{2} - 1\right) = \frac{p+1}{2} > \frac{p-1}{2}.$$

Through this, we see that the cases $v \equiv -2u \pmod p$ and $u \equiv -2v \pmod p$ both only occur when $u+v > \frac{p-1}{2}$. Therefore, if $u+v > \frac{p-1}{2}$ and $v \not\equiv -2u \pmod p, u \not\equiv -2v \pmod p$, then $[u:v], [u:u+v]$, and $[u+v:v]$ will correspond to the same relation under (1.3), so we can eliminate only one symbol from these triplets of symbols.

Putting this all together, we arrive at the following formula for counting the number of symbols necessary to generate $H_1(X_1(p), C_1^0, \mathbb{Z}_p)^+$:

$$\left(\begin{array}{c}\text{Number of}\\ \text{Symbols}\\ \text{Satisfying}\\ u<v\leq\frac{p-1}{2}\end{array}\right) - \left(\begin{array}{c}\text{Number of}\\ \text{Symbols with}\\ u+v\leq\frac{p-1}{2}\end{array}\right) - \frac{1}{3}\left(\begin{array}{c}\text{Number of}\\ \text{Symbols with}\\ u+v>\frac{p-1}{2}\end{array} - \begin{array}{c}\text{Number of}\\ \text{Symbols with}\\ u\equiv -2v \pmod p\end{array} - \begin{array}{c}\text{Number of}\\ \text{Symbols with}\\ v\equiv -2u \pmod p\end{array}\right).$$

4. Counting Symbols

To compute the dimension using the formula from the previous section we now need only to count the number of possible symbols which satisfy each of the listed conditions. In doing so we have the following cases:

(1) $\boldsymbol{u < v \leq \frac{p-1}{2}}$ **:** We have the following table detailing the number of possible choices for u given a fixed v:

v	Possible u's	Number of Choices
$\frac{p-1}{2}$	$1, 2, \ldots, \frac{p-1}{2} - 1$	$\frac{p-1}{2} - 1$
$\frac{p-1}{2} - 1$	$1, 2, \ldots, \frac{p-1}{2} - 2$	$\frac{p-1}{2} - 2$
$\vdots$	$\vdots$	$\vdots$
2	1	1

Hence, there are

$$\sum_{i=1}^{\frac{p-1}{2}-1} \frac{p-1}{2} - i = \frac{1}{8}(p-1)(p-3) \text{ symbols of this form.}$$

(2) $\boldsymbol{u+v \leq \frac{p-1}{2}}$ **:** Next, we examine the number of possible choices for v given a fixed u:

u	Possible v's	Number of Choices
1	$2, 3, \ldots, \frac{p-1}{2} - 1$	$\frac{p-1}{2} - 2$
2	$3, 4, \ldots, \frac{p-1}{2} - 2$	$\frac{p-1}{2} - 4$
3	$4, 5, \ldots, \frac{p-1}{2} - 3$	$\frac{p-1}{2} - 6$
$\vdots$	$\vdots$	$\vdots$

Clearly u must have an upper bound which is less than $\frac{p-1}{2} - 1$, since if $u = \frac{p-1}{2} - 1$, then $v = \frac{p-1}{2}$ and so $u + v > \frac{p-1}{2}$. To determine the upper bound we must consider two separate cases:

(2a) $\boldsymbol{p \equiv 1 \pmod 4}$ **:** If $p \equiv 1 \pmod 4$, then we know that $2 \Big| \frac{p-1}{2}$; however, we cannot have $u = \frac{p-1}{4}$. If this were the case, then v must be at least $\frac{p-1}{4} + 1$, which would then give $u + v > \frac{p-1}{2}$. On the other hand, if $u = \frac{p-1}{4} - 1$, then we could have $v = \frac{p-1}{4}$ which would indeed satisfy $u + v \leq \frac{p-1}{2}$. Hence, the maximum value for u in this case is $u = \frac{p-1}{4} - 1$, which gives two possible values for v, namely, $v = \frac{p-1}{4}$ and $v = \frac{p-1}{4} + 1$. Therefore, in this case there are

$$\sum_{i=1}^{\frac{p-1}{4}-1} \frac{p-1}{2} - 2i = \frac{1}{16}(p-1)(p-5) \text{ symbols of this form.}$$

(2b) $\boldsymbol{p \equiv 3 \pmod 4}$ **:** If $p \equiv 3 \pmod 4$, i.e., $2 \nmid \frac{p-1}{2}$ but $2 \Big| \frac{p-1}{2} - 1$, then we find the maximum value for u in this case is $u = \frac{p-1}{2} - 1 = \frac{p-3}{2}$, which corresponds to exactly one possible v, namely $v = \frac{p+1}{4}$. Thus, in this case there are

$$\sum_{i=1}^{\frac{p-3}{4}} \frac{p-1}{2} - 2i = \frac{1}{16}(p-3)^2 \text{ symbols of this form.}$$

(3) $\boldsymbol{u+v > \frac{p-1}{2}}$ **:** Similar to (2) we begin by examining the number of possible choices for u given a fixed v:

v	Possible u's	Number of Choices
$\frac{p-1}{2}$	$1, 2, \ldots, \frac{p-1}{2} - 1$	$\frac{p-1}{2} - 1$
$\frac{p-1}{2} - 1$	$2, 3, \ldots, \frac{p-1}{2} - 2$	$\frac{p-1}{2} - 3$
$\frac{p-1}{2} - 2$	$3, 4, \ldots, \frac{p-1}{2} - 3$	$\frac{p-1}{2} - 5$
$\vdots$	$\vdots$	$\vdots$

Next we need to determine a lower bound on v, and we again must consider two cases:

(3a) $\boldsymbol{p \equiv 1 \pmod 4}$ **:** If $p \equiv 1 \pmod 4$, then $2 \Big| \frac{p-1}{2}$. Clearly we cannot have $v = \frac{p-1}{4}$, since in this case there would be no $u < v$ which would

give $u+v > \frac{p-1}{2}$. However, if $v = \frac{p-1}{4}+1$, then $u = \frac{p-1}{4}$ is the only possible choice. Thus, we find

$$\frac{p-1}{4}+1 \leq v \leq \frac{p-1}{2},$$

which gives $\frac{p-1}{4}$ possible v's. Hence, there are

$$\sum_{i=1}^{\frac{p-1}{4}} \frac{p-1}{2} - (2i-1) = \frac{1}{16}(p-1)^2 \text{ symbols of this form.}$$

(3b) $\boldsymbol{p \equiv 3 \pmod 4}$ **:** If $p \equiv 3 \pmod 4$, then $2 \nmid \frac{p-1}{2}$; however, $2 \Big| \frac{p-1}{2}+1$. If we take $v = \frac{p+1}{4}$, then we must have $u \geq \frac{p+1}{4} - 1 = \frac{p-3}{4}$ for the inequality $u+v > \frac{p-1}{2}$ to occur. However, in this case we would then have $u > v$ which is impossible. Thus, the lower bound for v will be $v = \frac{p+1}{4}+1 = \frac{p+5}{5}$ which gives two possible values for u, namely, $u = \frac{p-3}{4}, \frac{p+1}{4}$. Thus,

$$\frac{p+5}{4} \leq v \leq \frac{p-1}{2},$$

giving $\frac{p-3}{4}$ possible v's. Hence, there are

$$\sum_{i=1}^{\frac{p-3}{4}} \frac{p-1}{2} - (2k-1) = \frac{1}{16}(p+1)(p-3) \text{ symbols of this form.}$$

(4) $\boldsymbol{u \equiv -2v \pmod p}$ **:** We first note that since we require $u < v \leq \frac{p-1}{2}$, the condition $u \equiv -2v \pmod p$ is equivalent to the condition $u+2v = p$. With this in mind we see that there is only one possible choice for u given a fixed v:

v	$2v$	u
$\frac{p-1}{2}$	$p-1$	1
$\frac{p-1}{2}-1$	$p-3$	3
$\vdots$	$\vdots$	$\vdots$
$\frac{p-1}{2}-i$	$p-1-2i$	$2i+1$

Once again we need to determine a lower bound for v, which is equivalent to determining an upper bound on i. Since we need $u < v$, we have that

$$2i+1 < \frac{p-1}{2} - i,$$

which can be rewritten as

$$3i \leq \frac{p-5}{2}.$$

Now we must consider the following cases:

(4a) $\boldsymbol{p \equiv 2 \pmod 3}$ **:** If $p \equiv 2 \pmod 3$, then $3 \Big| \frac{p-5}{2}$ so that $i \leq \frac{p-5}{6}$. Taking i to be largest, $i = \frac{p-5}{6}$, we find that $v = \frac{p+1}{3}$ and $u = \frac{p-2}{3}$. Hence, for $i = 0, \ldots, \frac{p-5}{6}$, i.e., for $v = \frac{p-1}{2}, \ldots, \frac{p-1}{2} - \frac{p-5}{6} = \frac{p+1}{3}$ we will have a corresponding u which satisfies our equality. Hence, there are

$$\frac{p-5}{6}+1 = \frac{p+1}{6} \text{ symbols of this form.}$$

(4b) $p \equiv 1 \pmod 3$ **:** If $p \equiv 1 \pmod 3$, then $3 \nmid \frac{p-5}{2}$, so we cannot have equality in $3i \leq \frac{p-5}{2}$, i.e., we must have $3i < \frac{p-5}{2}$, or equivalently, $3i \leq \frac{p-5}{2} - 1 = \frac{p-7}{2}$. Now, we have $3 \Big| \frac{p-7}{2}$ and so $i \leq \frac{p-7}{6}$. Again, taking the largest i, $i = \frac{p-7}{6}$, we find that $v = \frac{p+2}{3}$ and $u = \frac{p-4}{3}$. So, for $i = 0, \ldots, \frac{p-7}{6}$, i.e., for $v = \frac{p-1}{2}, \ldots, \frac{p-1}{2} - \frac{p-7}{6} = \frac{p+2}{3}$ we will have a corresponding u which satisfies our equality. Hence, there are

$$\frac{p-7}{6} + 1 = \frac{p-1}{6} \text{ symbols of this form.}$$

(5) $v \equiv -2u \pmod p$ **:** As in case (4), this condition is equivalent to the condition $2u + v = p$. Clearly, if $p = 5$ there are no solutions, since our only options are $u = 1, v = 2$, so we may assume here that $p \geq 7$. In this case, we must determine both upper and lower bounds for u. To begin we will determine the upper bound, so we note that $v = p - 2u$, and since $u < v$ it follows that $3u < p$, or equivalently, $3u \leq p - 1$. With this we have two cases to consider:

(5a) $p \equiv 1 \pmod 3$ **:** If $p \equiv 1 \pmod 3$, then $3 \Big| p - 1$ so that $u \leq \frac{p-1}{3}$. Taking u to be largest, $u = \frac{p-1}{3}$ we find that $v = \frac{p+2}{3}$ (we also note here that since $p \geq 7$ in this case, u and v indeed satisfy $u < v \leq \frac{p-1}{2}$), so $u \leq \frac{p-1}{3}$.

(5b) $p \equiv 2 \pmod 3$ **:** If $p \equiv 2 \pmod 3$, then $3 \nmid p - 1$, so we must have $3u < p - 1$, or equivalently, $3u \leq p - 2$. Since $3 \Big| p - 2$, it follows $u \leq \frac{p-2}{3}$. Again taking u to be largest we note that $u = \frac{p-2}{3}$ has a corresponding $v = \frac{p+3}{4}$ (which again satisfies $u < v \leq \frac{p-1}{2}$ since $p > 5$). Hence, $u \leq \frac{p-2}{3}$.

Next, we must determine the lower bound for u. We still have $v = p - 2u$, and since $v \leq \frac{p-1}{2}$ it follows that $\frac{p+1}{2} \leq 2u$. Again, we have two cases to consider:

(5c) $p \equiv 3 \pmod 4$ **:** If $p \equiv 3 \pmod 4$ then $2 \Big| \frac{p+1}{2}$ so that $\frac{p+1}{4} \leq u$. Taking the minimal u then gives $u = \frac{p+1}{4}$ so $v = \frac{p-1}{2}$ which clearly satisfies $u < v \leq \frac{p-1}{2}$. Hence, $\frac{p+1}{4} \leq u$.

(5d) $p \equiv 1 \pmod 4$ **:** If $p \equiv 1 \pmod 4$ then $2 \nmid \frac{p+1}{2}$ so that $\frac{p+1}{4} < u$, or equivalently, $\frac{p+1}{4} + 1 \leq 2u$, i.e., $\frac{p+3}{2} \leq 2u$. Since $4 \Big| p + 3$, we then have $\frac{p+3}{4} \leq u$. The minimal u is now $u = \frac{p+3}{4}$ which has a corresponding $v = \frac{p-3}{2}$ and satisfies $u < v \leq \frac{p-1}{2}$ (we note here that $p \neq 5$ is crucial). Hence, $\frac{p+3}{4} \leq u$.

Combining the above, we then have the following four cases for the bounds of u, which subsequently also gives the number of possible symbols (since each u corresponds to exactly one v):

(5e) $p \equiv 1 \pmod{12}$ **:** (Cases (5a)+(5d))

$$\frac{p+3}{4} \leq u \leq \frac{p-1}{3} \text{ giving } \frac{1}{12}(p-1) \text{ symbols of this form.}$$

(5f) $p \equiv 5 \pmod{12}$ **:** (Cases (5b)+(5d))

$$\frac{p+3}{4} \leq u \leq \frac{p-2}{3} \text{ giving } \frac{1}{12}(p-5) \text{ symbols of this form.}$$

(5g) $\boldsymbol{p \equiv 7 \pmod{12}}$ **:** (Cases (5a)+(5c))

$$\frac{p+1}{4} \leq u \leq \frac{p-1}{3} \text{ giving } \frac{1}{12}(p+5) \text{ symbols of this form.}$$

(5h) $\boldsymbol{p \equiv 11 \pmod{12}}$ **:** (Cases (5b)+(5c))

$$\frac{p+1}{4} \leq u \leq \frac{p-2}{3} \text{ giving } \frac{1}{12}(p+1) \text{ symbols of this form.}$$

5. Results

Finally, we combine results found in Section 2 with the formula from Section 3 to determine the number of generators in the following four possible cases:

- $\boldsymbol{p \equiv 1 \pmod{12}}$ **:**

$$\frac{1}{8}(p-1)(p-3)-\frac{1}{16}(p-1)(p-5)-\frac{1}{3}\left(\frac{1}{16}(p-1)^2-\frac{p-1}{6}-\frac{1}{12}(p-1)\right)=\frac{1}{24}(p^2-1)$$

- $\boldsymbol{p \equiv 5 \pmod{12}}$ **:**

$$\frac{1}{8}(p-1)(p-3)-\frac{1}{16}(p-1)(p-5)-\frac{1}{3}\left(\frac{1}{16}(p-1)^2-\frac{p+1}{6}-\frac{1}{12}(p-5)\right)=\frac{1}{24}(p^2-1)$$

- $\boldsymbol{p \equiv 7 \pmod{12}}$ **:**

$$\frac{1}{8}(p-1)(p-3)-\frac{1}{16}(p-3)^2-\frac{1}{3}\left(\frac{1}{16}(p+1)(p-3)-\frac{p-1}{6}-\frac{1}{12}(p+5)\right)=\frac{1}{24}(p^2-1)$$

- $\boldsymbol{p \equiv 11 \pmod{12}}$ **:**

$$\frac{1}{8}(p-1)(p-3)-\frac{1}{16}(p-3)^2-\frac{1}{3}\left(\frac{1}{16}(p+1)(p-3)-\frac{p+1}{6}-\frac{1}{12}(p+1)\right)=\frac{1}{24}(p^2-1)$$

Thus, we see that for any prime $p \geq 5$, the number of Manin symbols which generate $H_1(X_1(p), C_1^0, \mathbb{Z}_p)^+$ is $\frac{1}{24}(p^2-1)$.

References

[Sha06] R. Sharifi, *Modular symbols and Milnor K_2*. `http://math.arizona.edu/~sharifi/milnork2.pdf`, 2006.

[Shi71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.

Department of Mathematics, The University of Arizona, Tucson, AZ 85743
E-mail address: `rwilliams@math.arizona.edu`